Anti-Spam Compliance: How to Comply With the New Anti-Spam Law

Robert V. Hale, Esq.
Providian Financial Corporation
Val D. Hornstein, Esq.
Hornstein Law Offices

Overview

- Enacted on January 1, 2004, the U.S. “CAN-SPAM” Act – “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003” -- regulates the sending of unsolicited commercial e-mail by requiring anyone sending certain e-mail messages to take specific steps or face penalties of up to $2 million.

- This presentation reviews the federal law, as well as non-preempted California requirements, and how to comply with both.

Overview

- CAN-SPAM makes it *legal* to send unsolicited commercial e-mail, provided that the sender:
  - Does not disguise the source and nature of the e-mail;
  - Does not misappropriate resources in sending the e-mail; and
  - Gives recipients a meaningful way to avoid receiving future mailings.

Overview

- The Act applies to e-mail whose “primary purpose” involves advertising or promoting a commercial product or service, including content on a Web site.
- A "transactional or relationship message" – email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship – may not contain false or misleading header information, but otherwise is exempt from most provisions of the CAN-SPAM Act.
- Neither the meaning of “primary purpose” nor "transactional or relationship message" is clear at this time.
- The Act preempts state laws that expressly regulate the use of e-mail to send commercial messages, except to the extent that such laws prohibit the sending of false or deceptive e-mail messages.

Criminal Offenses

Sec. 4 of the CAN-SPAM Act prohibits the following activities (as criminal offenses in sending commercial e-mail messages):

- Using another computer without authorization and sending commercial email from or through it
  - "Computer" means either a computer used by the U.S. Government or a computer connected to the Internet – essentially any computer. This definition includes computers located outside the U.S., as long as the computer is used in a manner that affects interstate commerce or foreign commerce.
- Using a computer to relay or retransmit multiple commercial email messages to deceive or mislead recipients or an Internet access service about the origin of the message

Criminal Offenses

Sec. 4 of the CAN-SPAM Act prohibits the following activities (as criminal offenses in sending commercial e-mail messages) Continued:

- Falsifying header information in multiple email messages and initiating the transmission of such messages
- Registering for multiple email accounts or domain names using information that falsifies the identity of the actual registrant
- Falsely representing oneself as an owner of multiple Internet Protocol addresses that are used to send commercial email messages.

Civil Violations

The Act also establishes civil violations. Section 5(a) includes the following prohibitions and affirmative requirements:

- False or Misleading Header Information
- Deceptive Subject Headings
- Opt-Out Opportunity
- No Additional Messages After Out-Opt
- Other Required Content
- Aggravating Activities
- Sexually Oriented Material

False or Misleading Header Information

The Act prohibits materially false or misleading header information in a commercial e-mail message or a transactional or relationship message. Header information is considered materially false or misleading if:

(a) It includes an originating e-mail address, domain name, or IP address that was fraudulently acquired;

(b) It disguises the identity of the computer from which it originated; or

(c) The “from” line does not accurately identify the initiator of the message.

False or Misleading Header Information

- The difference between *falsifying* header information (a crime) and *misleading* header information is not clear at this time.

- If you send commercial e-mail from your own server, make sure the IP address listed in your e-mail header has a valid “Reverse DNS Lookup” associated with your domain name. You can check the reverse lookup of your IP address for free at DNSstuff.com

False or Misleading Header Information

- If you send commercial e-mail through an e-mail distribution service, place your company name and e-mail address in the “from” line. Most services offer this feature.

- Make sure that everyone in your company has their e-mail accounts properly configured in their e-mail client and their outgoing messages list their full name and e-mail address in the “from” line.

Deceptive Subject Headings

The Act prohibits a person from initiating the transmission of a commercial e-mail message if that person has or should have actual knowledge that the subject heading of the message would be likely to mislead the recipient about a material fact regarding the contents of the message.

Deceptive Subject Headings

- Remember, even if you unknowingly mislead recipients, you may still be liable if under the circumstances a reasonable person would find the subject line materially misleading.

- Appoint someone to review and approve subject headings for bulk mailings.

- Test subject lines.

Opt-Out Opportunity

The Act requires that commercial e-mail messages include a clear and conspicuous opportunity for recipients to opt out of receiving future commercial e-mail messages from the sender. The opt-out mechanism may be:

(1) A functioning e-mail address to which the recipient may send an opt-out reply; or

(2) A hyperlink to a menu listing types of commercial e-mail messages sent by the sender, with an opportunity for the recipient to affirmatively indicate on such menu the types of messages he or she does not want to receive

No Additional Messages After Opt-Out

- The Act prohibits the sender from sending another commercial e-mail more than 10 days after the recipient has opted out.

- The sender is also prohibited from disclosing with any other party the e-mail address of a recipient who has opted out.

Opt-Out Issues and Pointers

- Watch-out for:
  - Increased frequency of e-mails to subscribers.
  - Stand alone promotional messages.

- Allow your reply address to function as an unsubscribe mechanism.
  - Until the courts or the FTC clarify:
    - What “clear and conspicuous” means; and
    - How to ensure that a consent form requires an “affirmative action.”
  - If used as an unsubscribe mechanism, a return address must remain functional for 30 days after the message is sent.

- Check unsubscribe requests once a week to avoid noncompliance with 10 day rule.

Opt-Out Issues and Pointers

- Implement and maintain a database of opt-out e-mail address. Opt-out databases for a division are acceptable if the Company keeps divisions entirely separate.
  - But proceed with caution!
- Scrub your list against the opt-out database.
- When obtaining an e-mail list, understand the restrictions and get clear permission to use in the desired way.
- Recognize that spam opt-out does not bar non-commercial e-mails, letters, faxes, or phone calls (though other laws apply!).

Other Required Content

The Act also requires commercial e-mail messages to contain:

(1) A clear and conspicuous identification that the message is an advertisement or solicitation (unless the recipient has given prior consent to receive such messages); and

(2) The sender's valid physical postal address.

Other Required Content

- Until the courts or the FTC address the scope of affirmative consent, always comply with the identification requirement.
- Create a standardized identifier for your company and include it at the top of your messages. The Act does not currently require that the subject line include the identifier.
  - You may want to avoid using “ADV” in the subject line because most spam filters will block messages that use this abbreviation.

Other Required Content

- Until the courts or the FTC indicate whether post office boxes will suffice for the “physical address” requirement, use a street address or rent a virtual address.

- Since the Act applies to even a lone commercial e-mail message, require all employees to place a company-approved signature containing your street address at the end of every e-mail message they send.

Aggravating Practices

The CAN-SPAM Act also prohibits certain practices that aggravate the violations described above, including engaging in any of the following acts in connection with the above violations:

- Address harvesting – Programs that copy e-mail addresses from web pages, newsgroups, chat rooms, message boards, and online directories for web pages, instant message users, domain names, resumes, and dating services.
- Dictionary attacks – Programs that open a connection to the target mail server and then rapidly submit millions of random e-mail addresses. Many of these addresses have slight variations, such as "jdoe1abc@hotmail.com" and "jdoe2def@hotmail.com." The software then records which addresses are "live" and adds the addresses to the spammers list. These lists are typically resold to many other spammers.

Aggravating Practices

- Automated e-mail account creation

- Sending commercial e-mail to an e-mail account that the initiator knows, or should have known:

  (1) Was harvested from a third party's website or online service without authorization or;

  (2)Was generated through an automated process of combining words, letters, or numbers into different e-mail addresses.

Sexually Oriented Material

- Senders of commercial e-mail messages containing sexually oriented material have a separate set of requirements with which they must comply.

Businesses Promoted by False or Misleading Header Information

Section 6 of the Act prohibits a person or entity from promoting, or allowing the promotion of, that person's or entity's goods or services through the use of commercial e-mail that includes false or misleading header information (as described above), if the person or entity:

(1) Knows or should have known that its goods or services are being promoted in such an e-mail;

(2) Received or expected to receive an economic benefit from the promotion, and;

(3) Took no reasonable action to prevent such e-mails or detect such e-mails and report them to the FTC.

Businesses Promoted by False or Misleading Header Information

- Viral Marketing?: Whether a marketer is considered a “sender” when the marketer asks one consumer to forward a message to another consumer.
- Affiliate Marketing?: Whether a business that induces its affiliates to send out marketing materials on the marketer’s behalf is considered a “sender.”
  - May avoid liability for actions of affiliate if affiliate holds itself out as a separate line of business or a separate division.

Suits Under the Can-Spam Act

- Who Can Sue
  - The Act empowers various federal agencies, including the FTC, to bring enforcement actions under the Act
  - In addition, states and internet access services providers (i.e. ISPs) may, with certain exceptions, sue violators of the CAN-SPAM Act.
  - The Act does not provide for a general private cause of action.
    - However, the Act does not fully pre-empt state law in this respect and California's anti-spam law does provide for a private cause of action.
    - The Act does promote a "bounty" rewards approach.

Suits Under the Can-Spam Act

- Potential Damages
  - Injunctive relief
  - Actual monetary loss
  - Statutory damages
    - Calculated by multiplying the number of violations by up to $250 (and up to $100 for ISPs), with each piece of e-mail considered a separate violation.
    - Capped at $2M (or $1M for ISPs), but may be increased if aggravating circumstances apply. No caps for materially false or misleading header violations.

Who Can Be Sued

CAN-SPAM applies to:

- Person or entity sending a commercial e-mail message (i.e. the “initiator”)
- Person or entity advertising in a commercial e-mail message (i.e. the business on whose behalf the initiator is sending the e-mail)
- Each party may be considered an initiator under the Act and should comply with all aspects.
  - What happens when you run an e-mail advertisement on a third-party list, and the recipient requests removal?

Current CAN-SPAM Suits

- FTC v. Global Web Promotions Pty Ltd., et al. (April 28, 2004)
- FTC v. Avatar Nutrition LLC, et al. (April 23, 2004) (*see handout*)
- U.S. v. Daniel J. Lin et al. (April 23, 2004)
- America Online, Inc. v. John Does 1-40 (March 9, 2004)
- America Online, Inc. v. Davis Wolfgang Hawke, et al. (March 9, 2004)
- Earthlink, Inc. v. John Does 1-25, et al. (March 9, 2004)
- Microsoft Corp. v. JDO Media, Inc., et al. (March 9, 2004)
- Microsoft Corp. v. John Does 1-50 d/b/a Super Viagra Group (March 9, 2004)
- Yahoo!, Inc. v. Eric Head, et al. (March 9, 2004)
- Hypertouch, Inc. v. BVWebTies, LLC, BlueStream Media, and Does 1 to 10 (March, 4, 2004)

Forthcoming Regulations and Reporting Obligations

- FTC
  - By June 2004, a report to Congress that sets forth a timetable for establishing a nationwide “Do Not E-Mail” Registry.
  - By September 2004, a report to Congress that sets forth a reward system for individuals who supply information about violations of the CAN-SPAM Act.
  - By December 2004, rulemaking concerning the definition of “primary purpose,” transactional or relationship message, 10 day compliance period for opt-out requests, and additional aggravating practices.
  - By June 2005, a report to Congress that sets forth a plan to require commercial e-mail messages to be identifiable
- FCC
  - Promulgate rules governing the use of wireless e-mail devices and “mobile service commercial e-mail.

State Anti-Spam Regulation

- State laws may still "prohibit falsity and deception in any portion of a commercial electronic message or information attached thereto."
  - California's law bans all unsolicited commercial e-mail, unless the sender obtains prior permission or has a preexisting relationship. The CA law also provides a private right of action.

- Pre-2004 state laws remain in effect to the extent that they are directed to false or deceptive e-mail messages, and also those dealing with:
  - Trespass, fraud, theft (misappropriation/conversion), "little FTC acts"/unfair competition, state RICO laws, unjust enrichment, and other federal causes of action

General Compliance Tips

- Take a stringent approach to *all* CAN-SPAM and *all* non-preempted state law requirements until the courts and regulators clarify the gray areas.
- Establish a company policy against employees sending unapproved, unsolicited commercial e-mail to others. Incorporate this policy into the employee manual.
- Have counsel review all e-mail marketing campaigns and contracts.
  - In particular, such campaigns should employ only e-mail lists of recipients who have consented to receive such mailings.
  - Ensure that contracts address CAN-SPAM requirements.

General Compliance Tips

- Have counsel review client consent forms.
- Keep records of customers' consent and pre-existing business relationships with customers.
- Implement an anti-spam compliance program to train employees, monitor adherence and provide corrective action when necessary.

General Compliance Tips

- Collaborate with vendors (e-mail agents) on the best way to share opt-out lists.